

GDPR Compliance Checklist

- I understand what the GDPR is and the fines I will face if I do not comply

- Myself and any other staff members I have are all aware of the changes the GDPR will cause and have an understanding of how data protection law affects their work

- I have carried out an information audit into the personal data my business processes

- I have updated the privacy notices I give clients when collecting their data

- I have checked my processes and I know that I will be able to comply with individual's right to be informed

- I have checked my processes and I know that I will be able to comply with individual's right of access

- I have checked my processes and I know that I will be able to comply with individual's right to rectification

- I have checked my processes and I know that I will be able to comply with individual's right to erasure

- I have checked my processes and I know that I will be able to comply with individual's right to restrict processing

- I have checked my processes and I know that I will be able to comply with individual's right to data portability
- I have checked my processes and I know that I will be able to comply with individual's right to object to data processing
- I have checked my processes and I know that I will be able to comply with individual's right to not be subject to automated decision-making
- I have identified my business' lawful basis or bases for processing personal data and I have documented this both in my records and in the privacy notices I use
- I have reviewed the way that I ask for consent and know that it is in keeping with the GDPR rules
- I have reviewed the way that I ask children for consent in light of the new rules and I know that I am complying with the GDPR
- I know what a personal data breach is
- I understand the circumstances under which I must report a personal data breach to the ICO or/and to the individuals affected
- I understand what will happen if I don't report a personal data breach when I should have done so
- I understand what 'data protection by design and default' means and how it applies to new IT systems

- I know to conduct a 'Privacy Impact Assessment' if I will be using any new systems to process data

- I understand the circumstances under which I may need to appoint a data protection officer in my business

- I understand that if I have multiple establishments and some are abroad I will need to work out who my supervising authority is

- I know who to contact if I need more information about the GDPR